IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of: Thomas E. Creamer		Confirmation No.:	6219
Application No.	10/736,389	Examiner:	Noonan, Willow W.
Date filed:	December 15, 2003	Group:	2446

For: Authentication of mobile communication devices using mobile networks, SIP and Parlay

---

APPEAL BRIEF UNDER 37 C.F.R. § 41.37

Mail Stop Appeal Brief - Patents
Commissioner for Patents
P.O. Box 1450
Arlington, VA 22313-1450

Sir:

This Appeal Brief is being filed further to the Notice of Appeal which was filed on November 12, 2009. This Appeal Brief is being filed concurrently with a Petition for One-Month Extension of Time, and the Patent Office is expressly authorized to charge the extension fee and any other fees deemed necessary under 37 C.F.R. § 41.20(b) to Deposit Account No. 14-1437.

37 C.F.R. § 41.37(c)(1)(i) *Real Party in Interest*

The real party in interest is International Business Machines Corporation (IBM), the assignee of record. The assignment has been recorded by the USPTO on December 15, 2003, at Reel No. 014812, Frame No. 0691.

37 C.F.R. § 41.37(c)(1)(ii) *Related Appeals and Interferences*

No related appeals or interference proceedings are currently pending which would directly affect or be directly affected by or have a bearing on the Board's decision in this appeal.

37 C.F.R. § 41.37(c)(1)(iii) *Status of Claims*

Claims 1-3 and 25-30 are rejected and are being appealed.

37 C.F.R. § 41.37(c)(1)(iv) *Status of Amendments*

No claims were amended after the final Office action.

37 C.F.R. § 41.37(c)(1)(v) *Summary of Claimed Subject Matter*

Independent claim 1 of the instant application recites a method of authenticating a mobile communication device within a mobile network, which is a voice network, and a wireless network, which is a data network (see, for example, paragraph [0011], lines 1-4 of the specification and Fig. 1), the method comprising:

providing a mobile communication device configured to communicate over the mobile network and the wireless network, the mobile communication device including a

Session Initiation Protocol (SIP) user agent executing therein (see, for example, paragraph [0017], lines 1-5, and paragraph [0018], lines 3-6);

the mobile communication device receiving authentication data from a mobile service provider over the mobile network when the mobile communication device is within communication range of the mobile network (see, for example, paragraph [0020], lines 1-2, and Fig. 2);

the mobile communication device building a SIP referred by token using the authentication data received from the mobile service provider (see, for example, paragraph [0020], lines 2-4, and Fig. 2);

the mobile communication device sending the token to a SIP server via a wireless communications link over the wireless network (see, for example, paragraph [0022], lines 1-4, and Fig. 2);

the SIP server interpreting the token and forming a Parlay request for authentication using data specified by the token (see, for example, paragraph [0023], lines 1-2, and Fig. 2);

the SIP server sending the request for authentication of the mobile communication device to the mobile service provider (see, for example, paragraph [0023], lines 3-7, and Fig. 2);

the mobile service provider confirming or denying the request for authentication by sending a response to the SIP server (see, for example, paragraph [0025], lines 1-3, and Fig. 2);

the SIP server receiving the response from the mobile service provider and sending a reply to the mobile communication device over the wireless communications link indicating whether the request for authentication was confirmed (see, for example, paragraph [0025], lines 3-7, and Fig. 2); and

the mobile communication device receiving the reply from the SIP server (see, for example, paragraph [0025], lines 5-7).

Independent claim 25 of the instant application recites a system of authenticating a mobile communication device within a mobile network, which is a voice network, and a wireless network, which is a data network (see, for example, paragraph [0011], lines 1-4, and Fig. 1), the system comprising:

a mobile communication device configured to communicate over the mobile network and the wireless network, the mobile communication device including a Session Initiation Protocol (SIP) user agent executing therein (see, for example, paragraph [0017], lines 1-5, and paragraph [0018], lines 3-6);

a mobile service provider, wherein the mobile communication device receives authentication data from the mobile service provider over the mobile network when the mobile communication device is within communication range of the mobile network and builds a SIP referred by token using the authentication data received from the mobile service provider (see, for example, paragraph [0020], lines 1-4); and

a SIP server, wherein the mobile communication device sends the token to the SIP server via a wireless communications link over the wireless network, wherein the SIP server is configured to interpret the token and form a Parlay request for authentication using data specified by the token, and sends the request for authentication of the mobile communication device to the mobile service provider (see, for example, paragraph [0022], lines 1-4, and paragraph [0023], lines 1-7),

wherein the mobile service provider confirms or denies the request for authentication by sending a response to the SIP server, the SIP server receives the response from the mobile service provider and sends a reply to the mobile communication device over the wireless communications link indicating whether the request for authentication was confirmed (see, for example, paragraph [0025], lines 1-7).

Independent claim 28 of the instant application recites a machine-readable storage having stored thereon a computer program having a plurality of code sections, said code sections executable by a machine for causing the machine to perform a method of authenticating a mobile communication device within a mobile network, which is a voice network, and a wireless network, which is a data network (see, for example, paragraph [0011], lines 1-4, and Fig. 1), comprising the steps of:

providing a mobile communication device configured to communicate over the mobile network and the wireless network, the mobile communication device including a

Session Initiation Protocol (SIP) user agent executing therein (see, for example, paragraph [0017], lines 1-5, and paragraph [0018], lines 3-6);

the mobile communication device receiving authentication data from a mobile service provider over the mobile network when the mobile communication device is within communication range of the mobile network (see, for example, paragraph [0020], lines 1-2, and Fig. 2);

the mobile communication device building a SIP referred by token using the authentication data received from the mobile service provider (see, for example, paragraph [0020], lines 2-4, and Fig. 2);

the mobile communication device sending the token to a SIP server via a wireless communications link over the wireless network (see, for example, paragraph [0022], lines 1-4, and Fig. 2);

the SIP server interpreting the token and forming a Parlay request for authentication using data specified by the token (see, for example, paragraph [0023], lines 1-2, and Fig. 2);

the SIP server sending the request for authentication of the mobile communication device to the mobile service provider (see, for example, paragraph [0023], lines 3-7, and Fig. 2);

the mobile service provider confirming or denying the request for authentication by sending a response to the SIP server (see, for example, paragraph [0025], lines 1-3, and Fig. 2);

the SIP server receiving the response from the mobile service provider and sending a reply to the mobile communication device over the wireless communications link indicating whether the request for authentication was confirmed (see, for example, paragraph [0025], lines 3-7, and Fig. 2); and

the mobile communication device receiving the reply from the SIP server (see, for example, paragraph [0025], lines 5-7).

37 C.F.R. § 41.37(c)(1)(vi) ***Grounds of Rejection to be Reviewed on Appeal***

1. Whether claims 1, 3, 25, 27-28, and 30 are patentable over U.S. Published Patent Application 2004/0193712 to Benenati (hereinafter Benenati) in view of U.S. Published Patent Application 2003/0014668 to Faccin, *et al.* (hereinafter Faccin), and in further view of non-patent literature reference, "A Service Framework for Carrier Grade Multimedia Services Using Parlay APIs Over a SIP System" to Pailer (hereinafter Pailer) under 35 U.S.C. § 103(a).
2. Whether claims 2, 26, and 29 are patentable over Benenati in view of Faccin, further in view of Pailer, and further in view of AAPA under 35 U.S.C. § 103(a).

37 C.F.R. § 41.37(c)(1)(vii) ***Argument***

Claims 1, 3, 25, 27-28, and 30 are patentable over Benenati in view of Faccin, and in further view of Pailer under 35 U.S.C. § 103(a)

Independent claims 1, 25, and 28

Wireless networks are becoming increasingly prevalent with thousands of so called hotspots being deployed throughout the United States, Europe, and Asia. A hotspot refers to the coverage area surrounding a wireless access point within which a device can communicate wirelessly with the access point. The access point typically includes a wireless transceiver and is connected to a packet-switched communications network such as the Internet. As such, the access point provides network connectivity to those devices capable of establishing a wireless communications link with the access point. Mobile users can roam between multiple hot spots while maintaining connectivity with a communications network. Examples of hotspots or wireless networks can include those networks built around one of the 802 wireless communications protocols such as 802.11, 802.16, 802.20, and 802.15. Such wireless networks largely function independently of mobile communications networks. These wireless networks, particularly 802.11 wireless networks, often function purely as data networks. That is, typically voice communications are not carried over such networks. In consequence, the voice capability of mobile networks has yet to be integrated with 802.xx wireless networks. See Specification, paragraphs [0002]-[0003]. The present invention provides a method and system of authenticating a mobile communication device within a mobile network (a voice network) and a wireless network (a data network), and thus integrate these two types of networks.

Benenati discloses a method for common authentication and authorization (AA) between networks having disparate access technologies. A set of AA credentials from a user attempting to gain access to one of the networks may be received, and a subscriber database of another of the networks may be used to verify the set of AA credentials. A communication protocol common to the networks may be used. Additionally, the user may employ a single set of AA credentials, usable over multiple communication protocol layers. Further, a user may perform a single AA operation when roaming across two or more networks by gathering the user's key material during an AA challenge and reply session at a data link layer. The gathered material may be used for an AA challenge at an upper network layer or another network as the user transitions between networks. See the Abstract.

However, it is noted that in Benenati a set of AA credentials from a user may be used to gain access to multiple networks. In contrast, in the present invention, authentication data from a mobile service provider, not from a user, is used to gain access to a wireless network.

Benenati also does not disclose that the mobile communication device includes a Session Initiation Protocol (SIP) user agent executing therein and builds a SIP referred by token using the authentication data received from the mobile service provider. Benenati describes in paragraph [0039] that it may become possible for client software at the user to automatically supply the user's authentication credentials whenever the user moves between air interface technologies. However, Benenati does not disclose that the user's

authentication credentials are built into a SIP referred by token using the SIP user agent executing in the user device.

In fact, Benenati teaches away from running SIP on the user device (see paragraph [0034]: "If the user also runs IP Security (IPSec) or Session Initiation Protocol, an additional layer (Application layer) of authentication is also required. These multi-layer authentications may cause a data session to pause while the terminal is engaged in authentication requests, both upon initial connection and upon inter-technology handoff. This places a burden on the user and/or the client software and increases delays and provisioning complexities.").

Benenati further does not disclose the specific authentication steps occurred between the SIP server and the mobile service provider. More particular, Benenati does not disclose "the mobile communication device sending the token to a SIP server via a wireless communications link over the wireless network; the SIP server interpreting the token and forming a Parlay request for authentication using data specified by the token; the SIP server sending the request for authentication of the mobile communication device to the mobile service provider; and the mobile service provider confirming or denying the request for authentication by sending a response to the SIP server," as recited in independent claims of the instant application.

In summary, since Benenati's authentication scheme is totally different from that of the present invention, Benenati does not disclose the specific steps or limitations recited in independent claims 1, 25, and 28 of the instant application.

It was asserted in the final Office Action dated August 13, 2009 that Benenati teaches that the service provider may provide a key to an authentication client to be used in a future authentication process; thus Benenati does teach authentication credentials provided by a service provider. See Benenati at p. 4, paragraph 38 ("Upon verification of the signature the AAA entity authorizes (Step S340) the user 110 and may send (Step S350) a key for encryption and a new key material to be used in a future authentication process.").

However, it is noted that in Benenati the new key material to be used in a future authentication process is sent to the user. Thus, in the future authentication process the network obtains the new key material from the user in order to authenticate, and does not send a request for authentication to a provider in another network. In contrast, in the present invention the SIP server of the wireless network sends the request for authentication of the mobile communication device to the mobile service provider (not to the user) and the mobile service provider confirms or denies the request for authentication by sending a response to the SIP server.

Faccin and Pailer do not make up for the deficiencies of Benenati as discussed above. Although Faccin and Pailer mention the terms SIP protocol and Parlay respectively, they are not used in the context of present invention, namely authenticating a mobile communication device within a wireless data network using authentication data received from a mobile voice network, and no motivation or suggestion can be found in Benenati to combine those technologies with Benenati's invention.

Clearly, the cited references, alone or in combination, fail to disclose or suggest each and every element of independent claims 1, 25, and 28. Independent claims 1, 25, and 28 are, therefore, believed to be patentable over the cited references. All the dependent claims are believed to be patentable over the cited references because they are dependent on claims 1, 25, or 28.

Claims 3, 27, and 30

Claims 3, 27, and 30 are believed to be patentable because of their dependency on patentable independent claims 1, 25, and 28, respectively.

Claims 2, 26, and 29 are patentable over Benenati in view of Faccin, further in view of Pailer, and further in view of AAPA under 35 U.S.C. § 103(a).

Claims 2, 26, and 29

Claims 2, 26, and 29 are believed to be patentable because of their dependency on patentable independent claims 1, 25, and 28, respectively.

In view of the forgoing, the honorable Board is therefore respectfully urged to reverse the final rejection of the Primary Examiner.

Respectfully submitted,

NOVAK DRUCE + QUIGG LLP

Date: January 21, 2010

/Gregory A. Nelson/
Gregory A. Nelson, Registration No. 30,577
Yonghong Chen, Registration No. 56,150
525 Okeechobee Blvd., 15th Floor
West Palm Beach, FL 33401
Telephone: (561) 838-5229

37 C.F.R. § 41.37(c)(1)(viii) *Claims Appendix*

1. A method of authenticating a mobile communication device within a mobile network, which is a voice network, and a wireless network, which is a data network, the method comprising:

providing a mobile communication device configured to communicate over the mobile network and the wireless network, the mobile communication device including a Session Initiation Protocol (SIP) user agent executing therein;

the mobile communication device receiving authentication data from a mobile service provider over the mobile network when the mobile communication device is within communication range of the mobile network;

the mobile communication device building a SIP referred by token using the authentication data received from the mobile service provider;

the mobile communication device sending the token to a SIP server via a wireless communications link over the wireless network;

the SIP server interpreting the token and forming a Parlay request for authentication using data specified by the token;

the SIP server sending the request for authentication of the mobile communication device to the mobile service provider;

the mobile service provider confirming or denying the request for authentication by sending a response to the SIP server;

the SIP server receiving the response from the mobile service provider and sending a reply to the mobile communication device over the wireless communications link indicating whether the request for authentication was confirmed; and

the mobile communication device receiving the reply from the SIP server.

2. The method of claim 1, wherein the wireless network is compliant with at least one of an 802.16, 802.20, or 802.15 wireless communications protocol.

3. The method of claim 1, wherein the wireless network is compliant with an 802.11 wireless communications protocol.

25. A system of authenticating a mobile communication device within a mobile network, which is a voice network, and a wireless network, which is a data network, the system comprising:

a mobile communication device configured to communicate over the mobile network and the wireless network, the mobile communication device including a Session Initiation Protocol (SIP) user agent executing therein;

a mobile service provider, wherein the mobile communication device receives authentication data from the mobile service provider over the mobile network when the mobile communication device is within communication range of the mobile network and

builds a SIP referred by token using the authentication data received from the mobile service provider; and

a SIP server, wherein the mobile communication device sends the token to the SIP server via a wireless communications link over the wireless network, wherein the SIP server is configured to interpret the token and form a Parlay request for authentication using data specified by the token, and sends the request for authentication of the mobile communication device to the mobile service provider,

wherein the mobile service provider confirms or denies the request for authentication by sending a response to the SIP server, the SIP server receives the response from the mobile service provider and sends a reply to the mobile communication device over the wireless communications link indicating whether the request for authentication was confirmed.

26. The system of claim 25, wherein the wireless network is compliant with at least one of an 802.16, 802.20, or 802.15 wireless communications protocol.

27. The system of claim 25, wherein the wireless network is compliant with an 802.11 wireless communications protocol.

28. A machine-readable storage having stored thereon a computer program having a plurality of code sections, said code sections executable by a machine for causing the

machine to perform a method of authenticating a mobile communication device within a mobile network, which is a voice network, and a wireless network, which is a data network, comprising the steps of:

providing a mobile communication device configured to communicate over the mobile network and the wireless network, the mobile communication device including a Session Initiation Protocol (SIP) user agent executing therein;

the mobile communication device receiving authentication data from a mobile service provider over the mobile network when the mobile communication device is within communication range of the mobile network;

the mobile communication device building a SIP referred by token using the authentication data received from the mobile service provider;

the mobile communication device sending the token to a SIP server via a wireless communications link over the wireless network;

the SIP server interpreting the token and forming a Parlay request for authentication using data specified by the token;

the SIP server sending the request for authentication of the mobile communication device to the mobile service provider;

the mobile service provider confirming or denying the request for authentication by sending a response to the SIP server;

the SIP server receiving the response from the mobile service provider and sending a reply to the mobile communication device over the wireless communications link indicating whether the request for authentication was confirmed; and

the mobile communication device receiving the reply from the SIP server.

29. The machine-readable storage of claim 28, wherein the wireless network is compliant with at least one of an 802.16, 802.20, or 802.15 wireless communications protocol.

30. The machine-readable storage of claim 29, wherein the wireless network is compliant with an 802.11 wireless communications protocol.

37 C.F.R. § 41.37(c)(1)(ix) *Evidence Appendix*

None.

37 C.F.R. § 41.37(c)(1)(x) *Related proceedings Appendix*

None.